Online privatliv – udfordringer og mulige løsninger

Rikke Frank Jørgensen
Seniorforsker, Institut for Menneskerettigheder

Retten til privatliv er en af de menneskerettigheder, der er under særligt pres i det digitale domæne. Internettet ombryder og udfordrer grænser mellem offentlig og privat, og dets globale karakter gør det vanskeligt at gennemskue og kontrollere den stadigt stigende strøm af data der indsamles og udveksles mellem statslige og kommercielle aktører. Hvilke udfordringer står retten til privatliv over for? Og hvordan sikrer vi privatlivet i en digital tidsalder? Dette er to af de spørgsmål, som artiklen tager fat på.

Indledning

Det er efterhånden en triviel konstatering, at den digitale tidsalder har sat retten til privatliv under pres (Nissenbaum 2011, 140-147; Matzner 2014; Schneier 2015; United Nations General Assembly 2014). Edward Snowdens læk af dokumenter fra den amerikanske efterretningstjeneste, der startede i sommeren 2013, har illustreret mængden og omfanget af de personlige oplysninger, der kan tappes fra internettets infrastruktur og online services (Greenwald 2014). Snowdens afsløringer førte til vedtagelsen af de to første FN-resolutioner om Retten til Privatliv i en Digital Tidsalder, vedtaget på FN's Generalforsamling i 2013 og 2014 (United Nations General Assembly 2013; United Nations General Assembly 2014). Resolutionerne understreger blandt andet, at den stigende brug af kommunikationsteknologi forøger staters mulighed for at indsamle personoplysninger og overvåge borgere på måder, der krænker den enkeltes ret til privatliv. Som opfølgning på resolutionen i 2013 indsamlede FN's Højkommissær for menneskerettigheder oplysninger om nationale forhold og fremlagde i juni 2014 en rapport, der forholder sig meget kritisk til den praksis, der eksisterer i mange lande. Rapporten fremhæver blandt andet manglende transparens og retssikkerhed knyttet til statslig dataindsamling og overvågning (The Office of the United Nations High Commissioner for Human Rights 2014).

Snowden-sagen handler om efterretningstjenesters adgang til personoplysninger, men de aktuelle udfordringer for retten til privatliv er langt bredere end som så. Udfordringerne handler grundlæggende om, at personoplysninger i stigende grad anskues som et kommercielt råstof og om hidtil usete muligheder for at høste og udveksle dette råstof (Mayer-Schönberger & Cukier 2013; Lane et al. 2014; Matzner 2014).[1] Der er her en tæt kobling mellem mediets natur (det digitale format), brugen af personoplysninger og de udfordringer, det giver for privatlivet.

Såvel fra det politiske niveau, civilsamfundet, som den akademiske litteratur finder man bud på, hvorledes disse udfordringer kan imødegås. Forslagene grupperer sig typisk inden for tre hovedtilgange. Den første gruppe, som jeg kalder de retsoptimistiske, tager udgangspunkt i at styrke det eksisterende retlige paradigme for privatliv og databeskyttelse bl.a. med skærpede krav til information og samtykke (Bygrave 2002; Dix 2013; Kosta 2013). Kritikere af denne tilgang har fremhævet, at den overvurderer samtykkets betydning som beskyttelsesmekanisme, ikke mindst i forhold til online tjenester, hvor samtykket gives som en forudsætning for at bruge tjenesten (Solove 2012; Barocas & Nissenbaum 2014). Den anden gruppe, som jeg kalder de teknologioptimistiske, har fokus på teknologiens muligheder for at beskytte den enkelte gennem brug af *privacy*-fremmende teknologier og ved at indtænke databeskyttelse i systemer og forretningsgange gennem *privacy by design* (Information and Privacy Commissioner of Ontario and IBM Canada 2011; Rubenstein & Good 2013; Cristofaro & Murdoch 2014). Dette vil kræve, at nogle relativt overordnede principper omsættes

i konkrete løsninger, der indbefatter både IT-systemer, organisation og forretningsgange. Den tredje og sidste gruppe har jeg kaldt de kontekstradikale, fordi denne løsning er baseret på en grundlæggende gentænkning af online privatliv baseret på den kontekst, hvor data opsamles (Nissenbaum 2010; Nissenbaum 2011; Barth et al. 2006). Udfordringer er her, at løsningerne vil kræve, at en række statslige og kommercielle aktører skal viske tavlen ren og begynde at gøre tingene på en ny måde.

Jeg vil i artiklen argumentere for, at skal retten til privatliv overleve i en digital tidsalder, kræver det, at vi sætter ind på alle tre fronter samtidigt. Det retlige regime for databeskyttelse skal revideres, den organisatoriske kompetence skal styrkes, så privatliv og databeskyttelse i højere grad tænkes ind i systemer og forretningsgange, og der skal udvikles privatlivsmodeller, der er bæredygtige på længere sigt. Dette vil kræve en nuanceret forståelse af internettets særlige karakteristika som radikalt heterogent, socialt komplekst, og kontekstbrydende. Derudover er der brug for en kritisk stillingtagen til, hvad den klassiske opdeling mellem offentlig og privat betyder for rettigheder og pligter i det online domæne. En central pointe vil her være, at beskyttelsen af individets rettigheder i det digitale domæne er afhængig af, at vi eksplicit tager stilling til, hvilke normer der skal gælde for internettets infrastruktur og offentlige rum, uagtet at disse varetages af private aktører.

Artiklen indledes med en kort gennemgang af retten til privatliv og de udfordringer, som internettet og den digitale teknologi har givet beskyttelsen af privatlivet. Dernæst diskuteres tre hyppigt fremførte løsningsmodeller for en stærkere privatlivsbeskyttelse på internettet; en styrkelse af det retlige regime, en styrkelse på teknisk og organisatorisk niveau (privacy by design), og en gentænkning af persondatabeskyttelse med udgangspunkt i den specifikke kontekst. Afslutningsvis peges på en mulig vej fremad, herunder de politiske implikationer af denne.

Online privatliv under pres

Retten til privatliv (på engelsk '*privacy*') er en menneskerettighed, der følger af FN's Verdenserklæring om Menneskerettigheder fra 1948. Verdenserklæringens artikel 12 slår fast, at „ingen må være genstand for vilkårlig indblanding i private forhold, familie, hjem eller korrespondance, ej heller for angreb på ære og omdømme. Enhver har ret til lovens beskyttelse mod sådan indblanding eller angreb" (United Nations 1948, Article 12). En række internationale konventioner indeholder lignende bestemmelser, der beskytter privatlivet, herunder FN's konvention om civile og politiske rettigheder og Den Europæiske Menneskerettighedskonvention. Retten til privatliv er ikke absolut, men indgreb skal følge menneskeretlige standarder, herunder have hjemmel i lov og udgøre en nødvendig og proportional foranstaltning. Staters pligt til at beskytte privatlivet gælder både 'offline' og online' som fastslået i den første FN-resolution om menneskerettigheder på internettet fra 2012 (United Nations Human Rights Council 2012).

Beskyttelsen af privatlivet gælder ikke kun i det private domæne, men er en ret, der følger individet – også når det bevæger sig rundt i det offentlige rum. Eksempelvis er der i de fleste lande lovgivningsmæssige grænser for, i hvilket omfang staten eller kommercielle aktører må overvåge borgere, selvom de befinder sig i det offentlige rum. „The right to privacy may not only be invoked in private relationships at home, but may also be perceived as a kind of private sphere which is inherent in the individual person and which accompanies the person when moving about" (Rehof 1999, 258). I det følgende fokuseres primært på de aspekter af retten til privatliv, der vedrører registrering og brug af oplysninger om den enkelte.

Privatlivsnormen har været genstand for omfattende forskning og udredning siden Warren og Brandeis' skelsættende artikel fra 1890 (Warren and Brandeis 1890), hvor retten til privatliv defineres som retten til at være i fred („the right to be let alone"). Det mest dominerende perspektiv har fokuseret på retten til privatliv som muligheden for kontrol; kontrol over, hvad andre ved om os (informationskontrol), kontrol over beslutninger, der vedrører os selv, og kontrol over et fysisk område. „Something is private when I am in a position to and have a right to control access to it – whether to data, to a home, to decisions or to ways of acting" (Rössler 2007, 27). Princippet om kontrol med egne data gennemsyrer EU's databeskyttelseslovgivning, hvor det konkret er udmøntet i et krav om samtykke. Ideen om kontrol gennem samtykke bygger på en antagelse om en oplyst borger, der bevidst vælger at afgive eller ikke afgive sine oplysninger til en given myndighed eller privat tjeneste. Som led i denne tænkning er der i stigende grad fokus på transparens og information, herunder information om vilkår og betingelser for dataopsamling og –udveksling.[2] Dette synes at bygge på en antagelse om, at hvis blot oplysningen af brugeren er tilstrækkelig klar og tilgængelig, vil denne have reelle valgmuligheder, og udgangspunktet for et oplyst samtykke er til stede. Nyere forskning peger imidlertid på, at denne rationelle tilgang til databeskyttelse ikke indfanger de særlige karakteristika, der knytter sig til online-tjenester. „Notice and consent remains a procedural mechanism divorced from the particularities of relevant online activity" (Nissenbaum 2011, 35). Dette skyldes blandt andet, at internettet udfordrer grænser og opdelingen i 'offentlig' og 'privat' med en række konsekvenser for den gældende regulering på området.[3]

Et af internettets karakteristika er måden, det ændrer vilkårene for henholdsvis offentligt og privat liv på. På internettet er brugerens færden og de oplysninger, der afgives, i udgangspunktet gemt, delelige, søgbare og med stor kommerciel værdi. At holde oplysninger private er derimod en udfordring, der kræver en ekstra indsats og brug af tekniske beskyttelsesværktøjer. Hvor det tidligere krævede en særlig indsats at træde ud af det private og ind i det offentlige domæne, er det i dag omvendt. På internettet er vi 'offentlige *by default*', og kun i begrænset omfang og med en særlig indsats kan det private rum opretholdes. Selv data fra kommunikationsformer, som vi traditionelt anser som private, såsom telefoner og e-mail, bliver i stigende grad gemt, udvekslet og brugt, eksempelvis begrundet i anti-terror lovgivning eller for at bekæmpe anden alvorlig kriminalitet som illustreret nedenfor. Dette hænger dels sammen med internettets digitale form (al færden afgiver et søgbart aftryk), men det er også udtryk for, at data har fået stadig større værdi, såvel kommercielt som i forhold til staters sikkerhedspolitik. Som understreget af blandt andet Boyd er det ikke kun et systems design, der bestemmer, hvor offentligt eller privat det er, men også dets placering i det bredere samfundsmæssige økosystem (Boyd 2014, 204-205). Eksempelvis var Facebook som udgangspunkt designet som et privat alternativ til Myspace, men her har udbredelsen og anvendelsen blandt en milliard brugere været med til at gøre det til en af internettets mest offentlige platforme.

E-mails er både teknisk og lovgivningsmæssigt defineret som privat kommunikation, men eksempelvis EU's omstridte logningsregler (opbevaring af trafikdata om kommunikationer foretaget via telefon eller e-mail) illustrerer, at når oplysninger er digitalt tilgængelige, vil det ofte afføde en efterspørgsel – i dette tilfælde fra det sikkerhedspolitiske system. Med logningsreglerne blev der således skabt et retligt grundlag for, at kommunikationsoplysninger fra samtlige borgere skal opbevares, på trods af at de som udgangspunkt tilhører et privat domæne, og at de pågældende borgere ikke er under mistanke.[4]

Dertil kommer, at internettet er kendetegnet ved en radikal heterogenitet bestående af en myriade af sociale og kommercielle praksisser, der i mange sammenhænge har uklare grænser i forhold til at være offentlige og/eller private. Sociale medier udgør for mange en social infrastruktur, men er samtidig en kommerciel tjeneste, der lever af at sælge annoncer baseret på brugerens præferencer; aflæst gennem de handlemønstre og oplysninger, som brugeren afgiver om sig selv. Det vil sige, at oplysninger, som brugeren afgiver i én kontekst (socialt samvær med venner), overføres og bruges i en anden kontekst (målrettede reklamer baseret på brugerens adfærd og præferencer). Den udbredte brug af sociale medier indebærer, at kontekster, der traditionelt har været opdelt (hjem/arbejde, skole/fritid, privat kommunikation/offentlige udtalelser, socialsfære/kommerciel sfære), i stigende grad smelter sammen (Marvick 2012, 379). Dette medfører, at brugerne skal manøvrere i rum, der repræsenterer en blanding af kontekster, og hvor hierarkier mellem forældre/børn, chef/medarbejdere osv. optræder som ikke-hierarkiske strukturer på brugerens 'vennelister'.[5] Disse karakteristika udfordrer beskyttelsen af privatliv på internettet – og den tilhørende persondatalovgivning – på flere fronter.

Udfordringer for den gældende regulering

EU's medlemsstater har siden 1995 været bundet af EU's persondatadirektiv (95/46/EC), der opstiller krav til såvel offentlige som private virksomheders behandling af personoplysninger.[6] Persondatalovgivningen er baseret på grundprincipper om, at bestemte datatyper er beskyttelsesværdige, nemlig oplysninger der direkte eller indirekte kan henføres til en person. Behovet for beskyttelse ses med andre ord iboende i bestemte datatyper. Disse personoplysninger må kun behandles i forhold til et på forhånd defineret mål; der skal være proportionalitet mellem formål og de indsamlede data, der skal indsamles så lidt som muligt, brugeren skal som udgangspunkt give samtykke, der skal være transparens omkring databehandlingen, og bestemte sikkerhedsforskrifter skal være overholdt. Mere grundlæggende kan man sige, at EU's persondatabeskyttelse er baseret på ideen om en klar sondring mellem oplysninger, der har krav på beskyttelse (personoplysninger), og oplysninger der ikke har.

Realiteten på internettet er imidlertid, at kompleksiteten og mængden af de data, der indsamles, er enorm (og ofte udgør en blanding af flere datatyper); at data indsamles på tværs af lande og meget forskellige kontekster; at brugen af data er langt bredere end det oprindelige formål; at der forekommer meget forskellige niveauer af sikkerhed; at der er ringe transparens ift. virksomheders og myndigheders praksis; og at samtykke gives som en forudsætning for at bruge en given tjeneste snarere end som et bevidst valg. Disse forhold udfordrer grundlæggende EU's persondatabeskyttelse som fremhævet af blandt andet EU's Artikel 29-arbejdsgruppe (Article 29 Data Protection Working Party 2013). Til trods for en stigende skepsis ved effektiviteten af de gældende databeskyttelsesregler er ideen om kontrol gennem samtykke fortsat udgangspunktet for den retlige regulering på området – også i den igangværende revision af reglerne.

Hertil kommer, at der ikke eksisterer fælles bindende standarder for databeskyttelse på internationalt niveau. OECD's retningslinjer for beskyttelse af privatliv og transnationale data flow, der har bred opbakning blandt

OECD-landene, bliver ofte fremhævet som retningsgivende, men er ikke bindende.[7] Europarådets Konvention nr. 108 repræsenterer en af de første standarder på området og har ligesom EU's regler gennemgået en omfattende revision, bl.a. for at tage højde for online tjenester. Konventionen er imidlertid kun bindende for Europarådets medlemsstater.[8] På FN-niveau medførte Snowdens afsløringer, at FN's Generalforsamling i 2013 vedtog den første Resolution om retten til privatliv i en digital tidsalder (United Nations General Assembly 2013). Denne blev i 2014 fulgt op af en ny og skærpet tekst, der blandt andet understreger, at retten til privatliv er under alvorligt pres i det online domæne, og at stater har en forpligtelse til at sikre at national lovgivning og praksis, der indvirker på retten til privatliv, lever op til internationale menneskeretlige standarder på området (United Nations General Assembly 2014). Der er dog her særligt fokus på statslig overvågning og mindre opmærksomhed på den kommercielle behandling af personoplysninger.

En yderligere udfordring knytter sig til det forhold, at størsteparten af internettets infrastruktur og basale tjenester (teknisk infrastruktur, informationssøgning, sociale netværk mv.) administreres af private virksomheder, hvoraf mange er amerikanske. Dette giver en række konkrete udfordringer i forhold til at håndhæve EU's persondatalovgivning, som illustreret ved flere sager mellem EU's Artikel 29-gruppe og internetvirksomheder som Microsoft og Google.[9] Samtidig rejser det et mere principielt spørgsmål om, hvilke standarder der skal gælde for private virksomheder, der varetager vigtige samfundsmæssige funktioner. Har Google fx frie rammer til at definere deres services, eller følger der særlige forpligtelser med, når man er i en markedsdominerende position, og ens services er tæt koblet med samfundets demokratiske liv?

Nyere forskning, der ser på internetvirksomheders menneskeretlige forpligtelser, har argumenteret for, at der kan stilles skærpede krav til virksomheder, som har mulighed for at påvirke demokratiske processer på måder, der traditionelt har været forbeholdt offentlige institutioner (Laidlaw 2012, 55). I forhold til internetvirksomheder sondres mellem mikro-gatekeepere (indholdsplatforme), autoritative gatekeepere (Facebook, Wikipedia, portaler) og makro-gatekeepere (internetudbydere, søgemaskiner), hvor makro-gatekeepere vurderes at have den største indflydelse på samfundets demokratiske liv (Laidlaw 2012, 62). Pointen er her, at varetagelsen af afgørende samfundsmæssige funktioner indebærer en særlig forpligtelse til at sikre, at man ikke indvirker negativt på individets rettigheder, herunder retten til privatliv, ytrings- og informationsfrihed. I og med en stor del af internettets infrastruktur og informationsdomæne styres af private virksomheder, er det afgørende at blive skarpere på, hvilke forventninger vi som samfund har til disse aktører, og hvilke muligheder vi har for at håndhæve rettigheder overfor private virksomheder.

Pligten til at beskytte menneskerettigheder hviler på staten, men der har de seneste år været et øget fokus på, hvorledes private virksomheder mere proaktivt kan sikre respekt for menneskerettigheder, herunder retten til privatliv. Grænsefladen mellem staters pligt til at beskytte og virksomheders ansvar for at respektere menneskerettigheder er beskrevet i FN's retningslinjer for menneskerettigheder og erhverv fra 2011 (United Nations Human Rights Council 2011). Det fremgår her, at virksomheder skal formulere eksplicitte politikker på området; skal sikre, at de ikke bidrager til menneskeretlige krænkelser gennem interne procedurer og rettidig omhu (*due diligence*); og skal sikre klagemulighed og hjælp i forbindelse med potentielle krænkelser, de har medvirket til. Retningslinjerne er ikke bindende, men har vundet bred tilslutning hos internetvirksomheder.[10]

Tre svar på udfordringerne

Som nævnt indledningsvis er der forskellige bud på, hvorledes retten til privatliv kan styrkes i det online domæne. Den første tilgang, som jeg har kaldt de *retsoptimistiske,* agiterer for en øget beskyttelse gennem en stærkere og mere tidsvarende retlig regulering. En hovedaktør her er EU-kommissionen, der siden 2011 har arbejdet på en omfattende retlig reform af persondatadirektivet, og som forventer at vedtage en ny forordning på området i 2015/16.[11] De nye EU-regler sigter mod at ensrette niveauet for databeskyttelse på tværs af EU's medlemsstater og repræsenterer derudover en række bestemmelser, der skal øge beskyttelsen af den enkelte borger, særligt ved brug af onlinetjenester. Eksempelvis skærpes kravene til samtykke, der åbnes for omfattende bøder til virksomheder, der overtræder reglerne, og der stilles krav om at databeskyttelse indarbejdes på både teknisk og organisatorisk niveau (*privacy by design* og *privacy by default*).[12] Forordningen er blevet fremhævet som et meget ambitiøst svar på de skitserede udfordringer og har da også mødt massiv modstand fra amerikanske industrilobbyister i Bruxelles (European Digital Rights 2011).

Den nye forordning er blandt andet blevet kritiseret for at ville medføre store administrative byrder, særligt over for mindre virksomheder. Som modsvar har blandt andet EU's Artikel 29-arbejdsgruppe fremhævet, at man i implementeringen vil basere sig på en risikomodel, hvor institutioners forpligtelser skalerer afhængig af mængden og følsomheden af de data, der behandles (Article 29 Data Protection Working Party 2014). Dette indebærer ikke en fravigelse af grundlæggende databeskyttelsesprincipper, men betyder, at man som led i en obligatorisk

konsekvensanalyse vurderer graden af risiko i den pågældende situation (Article 29 Data Protection Working Party 2014, 4). De reviderede EU-regler løser imidlertid ikke det grundlæggende problem, at brugere samtykker som en forudsætning for at bruge tjenester på internettet.

En af udfordringerne er her, at internettjenester er baseret på indsamling af personoplysninger, og at disse har værdi som aldrig før. Størsteparten af internettjenesterne tjener penge via markedsføring og dermed af at vide så meget som muligt om deres brugere. Den kommercielle værdi af tjenesten er med andre ord direkte proportional med de oplysninger, som tjenesten har adgang til. Internettjenester som Facebook og Google er gratis for brugerne, men i realiteten betaler brugerne med de oplysninger, der afgives. Oplysninger om brugerens aktiviteter og præferencer indgår som et essentielt element i forretningsmodellen hos de sociale platforme, og for brugeren kan prisen for ikke at deltage være en manglende adgang til det sociale fællesskab, som tjenesten repræsenterer (Bechmann 2014; Jørgensen 2014). En forudsætning for at kunne beskytte retten til privatliv i det online domæne er derfor, at man starter med at anerkende, at deling af personoplysninger er prisen for at få adgang til en lang række internettjenester. Dette begrænser reelt brugerens valgmuligheder; særligt i de situationer hvor tjenesten opleves som en væsentlig forudsætning for at være med i et fællesskab. Et studie blandt danske gymnasielever i 2013 vedrørende brug af sociale medier som Facebook fremhævede eksempelvis, at samtykke opfattes som en nødvendig forudsætning for at deltage i sociale netværk snarere end en reel valgmulighed (Jørgensen 2014). Der er således et stigende misforhold mellem ideen om en oplyst bruger, der gennem sit samtykke vælger at afgive oplysninger til et nøje defineret formål, og den praksis, hvorigennem data afgives og bruges på internettet. Som svar på denne udfordring har flere argumenteret for, at udgangspunktet for databeskyttelse skal være kontekstspecifikke normer, der angiver grænser for, hvilke oplysninger der må opsamles og deles.

Som repræsentant for denne alternative tilgang, som jeg har kaldt de *kontekstradikale*, står særligt Nissenbaum (2010; 2011) og teorien om kontekstuel integritet. Hovedpointen er her, at det er konteksten, der skal bestemme beskyttelsesbehovet snarere end en attribut, der er iboende i den enkelte information. Data udveksles i stigende grad mellem forskellige kontekster, og til en række forskellige formål og på måder der for den enkelte bruger er uigennemskuelige. Udgangspunktet er derfor, at der til enhver kontekst knytter sig normer om, hvad der er passende og upassende deling af information. Med udgangspunkt i disse normer – der vil være mere eller mindre formaliserede alt efter den konkrete kontekst – kan man opstille krav til virksomheder og myndigheders behandling af personoplysninger, således at det primære databeskyttelsesansvar defineres ud fra konteksten snarere end med udgangspunkt i brugerens samtykke. Et af argumenterne lyder, at den dominerende markedspladsmetafor baseret på antagelsen om det frie marked og den frie forbruger ikke er tilstrækkelig, når vi skal definere og håndhæve standarder for grundlæggende samfundsmæssige funktioner på internettet (Nissenbaum 2011, 42). I stedet må vi eksplicitere, at funktioner, der er centrale for samfundets demokratiske liv – såsom at give adgang til internettet, at formidle informationssøgning på internettet, at stille en social infrastruktur til rådighed – forventes at leve op til selvstændige kvalitetsnormer på linje med professionsstandarder knyttet til bestemte erhverv, uagtet hvorvidt disse funktioner varetages af offentlige eller private aktører.[13] Pointen er med andre ord, at vigtige samfundsfunktioner må styres af kvalitetsparametre, der rækker ud over et økonomisk rationale, og er forankret i normative standarder knyttet til grundlæggende rettigheder, herunder transparens og retssikkerhed.

Udfordringen ved Nissenbaums model er imidlertid, at det er svært at se, hvordan den skal implementeres i praksis. Hvem skal definere, hvilke regler der skal være gældende for hvilke kontekster; hvad med kontekster, der ikke er klart definerede eller afgrænsede? Skal de respektive normsæt udmøntes i lovgivning? Og hvem skal overse, at de faktisk overholdes. Hvor gældende databeskyttelse er baseret på et forenklet og rationelt syn på kontrol med personoplysninger, åbner den kontekstuelle model for en kompleksitet, som er svær at se omsat til praksis.

Et tredje tilgang, som jeg har kaldt den *teknologioptimiske*, advokerer for ideen om at indarbejde privatlivsbeskyttelse i teknisk og organisatorisk arkitektur gennem '*privacy by design*'. Begrebet '*privacy by design*' stammer oprindelig fra Ann Cavoukian, der er tidligere Informations- og *Privacy*-Kommissær i Ontario, og bygger på en antagelse om, at beskyttelse af persondata ikke alene kan løses ved overholdelse af regelsæt, men skal være en del af organisationens samlede måde at operere på (Cavoukian 2009; Information and Privacy Commissioner of Ontario and IBM Canada 2011). *Privacy by design* omfatter både IT-systemer, forretningsområder, fysisk design og internet-forbundne infrastrukturer og er baseret på syv grundprincipper. 1) Der sigtes mod at forebygge snarere end at afhjælpe. 2) Persondatasikkerhed skal være en standardindstilling. 3) Sikkerheden bygges ind i designet og arkitekturen af IT-systemer og forretningspraksis. 4) Alle legitime formål tilgodeses, således at der ikke skal vælges mellem adgang til data og sikkerhed. 5) Der sikres en sikker håndtering af dataelementers livscyklus fra start til slut. 6) Systemernes komponenter og funktioner forbliver

synlige og transparente for både brugere og udbydere, således at kontrol er mulig. 7) Løsninger bygger på respekt for personlige data og brugeren i centrum.[14]

I 2010 vedtog den globale sammenslutning af *privacy*-kommissærer på deres årlige konference den første resolution om *privacy by design* baseret på Cavoukins begreb.[15] *Privacy by design* optræder ligeledes i EU's udkast til en ny databeskyttelsesforordning; som et obligatorisk krav ved udvikling af IT-løsninger, der indebærer behandling af personoplysninger. På trods af, at begrebet har cirkuleret i mere end ti år, er der imidlertid begrænsede eksempler på, hvorledes det omsættes i konkrete IT-løsninger og forretningsgange. Begrebet er fortsat relativt vagt, og det vil kræve en mere udfoldet beskrivelse af minimumskrav, hvis/når det skal tjene som en brugbar teknisk og organisatorisk standard, der lever op til EU's persondatalovgivning. Som led i dette bør også forholdet mellem den dataansvarlige (som er den kategori, persondataloven opererer med) og den teknisk/organisatoriske ansvarlige for implementering af *privacy by design* præciseres.

Vi står således i en situation, hvor der er store udfordringer for online *privacy*. Der er ingen internationale regelsæt, og EU's regler, som globalt set repræsenterer den mest udbyggede regulering af databeskyttelse, er under kraftig revision og baserer sig fortsat på samtykke som en central kontrolmekanisme. Dette på trods af at der i stigende grad stilles spørgsmålstegn ved samtykkes værdi og effekt, særligt i forbindelse med online tjenester. Over for dette står alternative forslag til regulering af området; ikke mindst Nissenbaums forslag om en kontekstuel tilgang til databeskyttelse. Ideen om en mere differentieret regulering baseret på analyse af normer og standarder i forskellige situationer i modsætning til en *one-size-fits-all privacy*-tænkning virker som et fornuftigt modsvar til de aktuelle udfordringer, men samtidig er der som skitseret ovenfor en række ubesvarede spørgsmål, der gør det svært at se modellen omsat til praksis.

Veje fremad

Vi står i dag i en paradoksal situation, når det gælder retten til privatliv. På den ene side har der aldrig tidligere været så eksplicitte udmeldinger fra det internationale menneskeretlige system om, at retten til privatliv gælder online som offline. Dette er cementeret i FN resolutioner, af FN's Højkommissær for menneskerettigheder, af Europarådet, Den Europæiske Menneskerettighedsdomstol, EU-Domstolen osv. På den anden side er der meget få muligheder for at håndhæve retten til privatliv på internettet. Data indsamles fra en lang række offentlige og private aktører på tværs af landegrænser; der er begrænset overblik over eller kontrol med dataindsamlingen; brugere afgiver et rutinemæssigt samtykke til, at deres data indsamles; og privatlivspolitikker er svært tilgængelige og læses af et fåtal af brugerne.

Udfordringerne er således mange, hvilket betyder, at skal retten til privatliv overleve i en digital tidsalder, kræver det, at der sættes ind både i forhold til gældende regulering og organisatorisk praksis og (mere langsigtet) i udviklingen af bæredygtige *privacy*-modeller. Den nye EU-forordning er et skridt fremad i forhold til at sikre en retlig ramme, der i højere grad afspejler den sociale praksis på internettet. Forordningen indeholder tiltag, der sigter mod at styrke beskyttelsen af den enkelte bruger, herunder skærpede krav til de vilkår, hvorunder samtykket afgives, skærpede sanktioner over for virksomheder, der bryder lovgivningen, skærpet underretningspligt ved sikkerhedsbrud, der involverer personoplysninger, og krav om *privacy by design* hos såvel offentlige institutioner som private virksomheder. Sidstnævnte er en vigtig komponent i at få *privacy* integreret mere bredt i organisationen og de teknologiske løsninger, men vil samtidig kræve, at begrebet konkretiseres og gøres mere operationelt, så det reelt bliver muligt at vurdere, om en given løsning lever op til principperne eller ej. Et af de nuværende problemer er, at databeskyttelse og IT-systemer ofte behandles som enten juridiske eller tekniske emner frakoblet hinanden. Hvis retten til privatliv skal være en integreret del af praksis i institutioner og virksomheder, kræver det et tæt samspil mellem retlige standarder, forretningsgange og teknologiske løsninger. Der er her brug for konkrete diskussioner af og eksempler på *privacy by design*-løsninger; herunder synliggørelse af, hvilke forretningsgange der er implementeret, hvordan tekniske løsninger er udformet, hvilke kontrolmekanismer der er indført, hvordan overensstemmelse med persondatalov er etableret osv.[16]

Den reviderede EU-forordning og en mere udbredt brug af *privacy by design* ændrer imidlertid ikke på, at der er brug for en opdatering af *privacy*-normen, der i højere grad modsvarer internettets mix af offentlige og private rum, samt det faktum at private virksomheder i overvejende grad kontrollerer internettets centrale funktioner og infrastruktur. Dette bringer os tilbage til Nissenbaums begreb om kontekstuel integritet og argumentet om, at den rationelle *one-size-fits-all privacy*-tænkning, som er udgangspunktet for gældende regulering på området, ikke længere kan stå alene. Frem for at tage udgangspunkt i bestemte datatyper og eksempelvis diskutere, om metadata er personoplysninger eller ej, vil det betyde, at vi i højere grad skal tage udgangspunkt i de konkrete situationer, hvor data opsamles og udveksles. Dette vil indebære, at der fra politisk side tages eksplicit stilling til, hvilke retningslinjer der skal gælde i en given kontekst – uanset om det vedrører informationssøgning på internettet, kontrol af en offentlig ydelse eller en lægekonsulta-

tion. I praksis vil det betyde, at persondatalovgivningen, der overvejende har fokus på processuelle betingelser for dataindsamling og -udveksling, suppleres med substantielle anvisninger vedrørende, hvilke data der må opsamles og udveksles i en given kontekst. Det betyder eksempelvis, at en praktiserende læge ud over at skulle efterleve persondatalovens generelle principper også skal efterleve specifikke regler, der er udformet med udgangspunkt i 1) analyse af de involverede aktører, her læge og patient, 2) analyse af informationstype, her fortrolige sundhedsoplysninger, og 3) analyse af transmissionsprincippet, her oplysninger afgivet under samtykke under forudsætning af fortrolighed (Nissenbaum 2007, 140-147).

Dette vil indebære et omfattende analytisk/normativt arbejde med at fastslå og eksplicitere, hvilke normer der skal være retningsgivende i forskellige sociale kontekster, online som offline. For nogle kontekster vil en del standarder allerede eksistere (fx bankvæsen), mens andre kontekster – eksempelvis informationssøgning på internettet – vil kræve en analyse af sammenlignelige analoge eksempler (fx informationssøgning på biblioteker). Som tidligere nævnt er svagheden ved kontekstmodellen knyttet til implementeringen; ikke mindst det omfattende analytiske og politiske arbejde med at få fastslået og vedtaget standarder for '*appropiate data flows*' inden for en lang række samfundsfunktioner. Hertil kommer udfordringen med at afgrænse kontekster/situationer i et digitalt domæne, der blandt andet er kendetegnet ved at være kontekstbrydende.

En mulig vej frem kunne derfor være, at man som supplement til en EU's skærpede regler for databeskyttelse og *privacy by design* påbegynder nogle få afgrænsede pilotprojekter med udgangspunkt i kontekstmodellen. Dette vil give konkrete erfaringer med at kombinere det eksisterende retlige regime med substantielle standarder for databehandling inden for udvalgte områder. Samtidig kan det medvirke til, at der skabes en højere grad af transparens i forhold til, hvilke normer og regelsæt forskellige aktører forventes at efterleve. Som led heri kan man arbejde henimod at styrke det løbende tilsyn og kontrol med databeskyttelse ved at anmode virksomheder og institutioner om regelmæssigt at undergå en uafhængig revision af deres databeskyttelsespraksis med udgangspunkt i både persondatalovgivning (proces) og de fastlagte standarder.

Litteratur

Anderson, E 1995, *Value in Ethics and Economics*, Harvard University Press, Cambridge.

Article 29 Data Protection Working Party 2009 *Opinion 5/2009 on online social networking*, EC Justice, Bruxelles, 22. juni 2009.

Article 29 Data Protection Working Party 2013, *Opinion 03/2013 on purpose limitation*, EC Justice, Bruxelles.

Article 29 Data Protection Working Party 2014, *Statement on the role of a risk-based approach in data protection legal frameworks*, EC Justice, Brussels, 30 maj 2014.

Barocas, S & Nissenbaum, H 2014, 'Big Data's End Run around Procedural Privacy Protections', *Commun ACM Communications of the ACM*, vol. 57, no. 11, pp. 31-33.

Barth, A, Datta, A, Mitchell, JC & Nissenbaum, H 2006, *Privacy and Contextual Integrity: Framework and* Applications, IEEE Symposium on Security and Privacy, Berkeley/Oakland, maj 2006.

Bechmann, A 2014, 'Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook', *Journal of Media Business* Studies, vol. 11, no. 1, pp. 21-38.

Boyd, D 2014, *It's Complicated: The Social Lives of Networked Teens*, Yale University Press, New Haven.

Bygrave, LA 2002, *Data Protection Law. Approaching Its Rationale, Logic and Limits*, Kluwer Law International, Haag, London, New York.

Cavoukian, A 2009, *Privacy by Design, Take the Challenge*, Information and Privacy Commissioner of Ontario, Toronto.

Cristofaro, ED & Murdoch, SJ (red.) 2014, *Privacy Enhancing Technologies*, 14th International Symposium, PETS, Amsterdam, 16.-18. juli 2014.

Dix, A 2013, 'The Commission's Data Protection Reform After Snowden's Summer', *Intereconomics*, vol. 48, no. 5, pp. 268-285.

European Digital Rights 2011, US lobbying against draft Data Protection Regulation, EDRi, Bruxelles, 22. December 2011. Tilgået 21. maj 2015 på: https://edri.org/us-dpr/

European Union 1995, *Directive 95/46/EC of the European Parliament and of the Council*, European Union, Bruxelles, 24. oktober 1995.

European Union 2006, *Directive 2006/24/EC of the European Parliament and of the Council*, European Union, Bruxelles, 15. marts 2006.

Greenwald, G 2014, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*, Metropolitan Books, New York.

Hwang, T & Levy, K 2015, "The Cloud' and Other Dangerous Metaphors, *The Atlantic*, 20. januar 2015.

Information and Privacy Commissioner of Ontario and IBM Canada 2011, *Privacy by Design from Policy to Practice*, Information and Privacy Commissioner of Ontario, Canada, Toronto.

Irish Data Protection Commisioner 2012, *Report of RE-Audit*, Irish Data Protection Commisioner, Portarlington, 21. september 2012.

Jørgensen, RF 2014, 'The Unbearable Lightness of User Consent', *Internet Policy Review*, vol. 3, no. 4.

Kosta, E 2013, *Consent in European Data Protection Law*, Brill Nijhoff, Leiden.

Laidlaw, EB 2012, *Internet Gatekeepers, Human Rights, and Corporate Social Responsibility*, ph.d.-afhandling, London School of Economics and Political Science, London.

Lane, J, Stodden, V., Bender, S & Nissenbaum, H 2014, *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, Cambridge University Press, New York.

Marvick, AE 2012, 'The Public Domain: Social Surveillance in Everyday Life', *Surveillance & Society*, vol. 9, no. 4, pp. 378-393.

Matzner, T 2014, 'Why Privacy Is Not Enough Privacy in the Context of „Ubiquitous Computing" and „'Big Data"', *Journal of Information Communication and Ethics in Society*, vol. 12, no. 2, pp. 93-106.

Mayer-Schönberger, V & Cukier, K 2013, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, Boston.

Nissenbaum, H 2007, 'Privacy in Context', in G Stocker & C Schöpf (red.), *Goodbye privacy*, Ars Electronica 2007. Ostfildern-Ruit, Hatje Cantz Verlag.

Nissenbaum, H 2010, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books, Stanford.

Nissenbaum, H 2011, 'A Contextual Approach to Privacy Online', *Dædalus, the Journal of the American Academy of Arts & Sciences*, vol. 140, no. 4, pp. 32-48.

Rehof, LA 1999, 'Article 12', in G Alfredsson & A Eide (red.), *The Universal Declaration of Human Rights: A Common Standard of Achievement*, Martinus Nijhoff Publishers, Haag; Boston; Cambridge.

Rubenstein, IS & Good, N 2013, 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents', *Berkely Technology Law Journal*, vol. 28, no. 2.

Rössler, B 2007, 'The Value of Privacy', in G Stocker & C Schöpf (red.), *Goodbye privacy*, Ars Electronica 2007. Ostfildern-Ruit, Hatje Cantz Verlag.

Schneier, B 2015, *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World*, W. W. Norton & Company, New York.

Solove, D 2012, 'Privacy Self-Management and the Consent Dilemma', *Harvard Law Review*, vol. 126, pp. 1880-1903.

The Office of the United Nations High Commissioner for Human Rights 2014, *The Right to Privacy in the Digital Age*, United Nations, New York, 30. juni 2014.

United Nations 1948, *The Universal Declaration of Human Rights*, United Nations, New York.

United Nations General Assembly 2013, *Resolution adopted by the General Assembly. The Right to Privacy in the Digital Age*, United Nations, New York, 18. december 2013.

United Nations General Assembly 2014, *Resolution adopted by the General Assembly. The Right to Privacy in the Digital Age*, United Nations, New York, 19. november 2014.

United Nations Human Rights Council 2012, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, A/HRC/20/L.13, United Nations, Geneva, 5. juli 2012.

United Nations Human Rights Council 2011, *Report of the Special Representative John Ruggie. Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*, United Nations, New York, 21. marts 2011.

Warren, S & Brandeis, L 1890, 'The Right to Privacy', *Harvard Law Review*, vol. 4, no. 5.

Watson, SM 2015, 'Metaphors of Big Data', *DIS Magazine*, 20. februar 2015.

Weintraub, J 1997, 'The Theory and Politics of the Public/Private Distinction', in J Weintraub and K Kumar (red.), *Public and Private in Thought and* Practice, The University of Chicago Press, Chicago.

Noter

1. Som påpeget af bl.a. Watson (2015) og Hwang og Levy (2015) trækker meget af 'big data'-litteraturen på en råstofmetafor. Denne begrebsliggørelse af big data er med til at understrege data som noget, der kan udvindes og har kommerciel værdi, modsat hvis man fx talte om data som kropslige legemsdele.
2. Se for eksempel udtalelsen fra EU's ekspertgruppe på området, den såkaldte Artikel 29 arbejdsgruppe, vedrørende sociale medier og privatliv (Article 29 Data Protection Working Party 2009) og tilsynsrapporten fra det irske datatilsyn vedrørende Facebook (Irish Data Protection Commisioner 2012). Begge steder er der fokus på, at brugerne skal have bedre og mere tilgængelig information om, hvorledes deres data behandles som en forudsætning for at kunne samtykke.
3. Aktuelle politiske såvel som teoretiske diskussioner trækker på forskellige offentlig/privat-distinktioner med hver deres ideologiske ståsted, ofte uden at dette er eksplicitteret (Weintraub 1997, xiii). I det følgende henviser distinktionen offentlig/privat primært til opdelingen mellem individets private domæne (beskyttet gennem retten til privatliv) over for et statsligt eller kommercielt domæne.
4. EU's logningsdirektiv fra 2006 (2006/24/EC) blev i april 2014 kendt ugyldigt af EU-Domstolen. EU-Domstolen fandt, at direktivet krænker EU-borgeres ret til privatliv og beskyttelse af personoplysninger som fastlagt i EU's Charter for Grundlæggende Rettigheder, Artikel 7 og 8. Afgørelsen er tilgængelig på: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf
5. Det bemærkes dog, at der på mange sociale medier er mulighed for at angive relationstyper (fx familiemedlemmer), og derved reetablere dele af det sociale hierarki.
6. Som nævnt ovenfor er retten til privatliv blandt andet baseret på en præmis om, at der i relationen mellem individ og stat er behov for at beskytte en personlig zone (hjem, familie, oplysninger) og sætte grænser for statens råderum. EU's persondatalovgivning udmønter retten til privatliv og beskyttelsen af personoplysninger på lige fod over for det statslige og kommercielle domæne. Kravene til beskyttelse af personoplysninger – og de grænser der sættes for behandlingen af disse – gælder således (i en europæisk kontekst), uanset om databehandlingen varetages af en offentlig myndighed eller privat virksomhed.
7. OECD-retningslinjerne er tilgængelige på: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
8. Se http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm
9. Se http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htmm.
10. Se Global Network Initiative, der er et samarbejde mellem en række af de store internet virksomheder om at udmønte og efterleve normer, der lever op til internationale menneskeretlige standarder for ytringsfrihed og privatliv. Tilgængelig på www.globalnetworkinitiative.org.
11. Se http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
12. Jf. EU's udkast til databeskyttelsesforordning af 30. juni 2014, tilgængelig på: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010617%202014%20INIT
13. Nissembaum trækker her på Elizabeth Anderson (1995, 147).
14. En dansk version af privacy by design principperne er tilgængelig på: http://www.privacybydesign.ca/content/uploads/2013/02/7foundationalprinciples-danish.pdf
15. 32nd International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy by Design, October 2010, tilgængelig på: https://www.ipc.on.ca/site_documents/pbd-resolution.pdf
16. For et eksempel på konkret anvendelse af privacy by design se f.eks. Rubenstein og Good (2013), der anvender Cavoukians principper til at analysere ti privacy hændelser hos Google og Facebook.